SEGURIDAD EN LA VIRTUALIZACIÓN: COMPRENDER LA DIFERENCIA

Kaspersky Security for Virtualization

KASPERSKY lab

Seguridad en la virtualización: comprender la diferencia

¿Ya está virtualizando los activos de hardware? En ese caso, lo más seguro es que su objetivo empresarial sea el de obtener la máxima eficiencia de su infraestructura de IT. Ejecutar varias máquinas virtuales (VM) a la vez en un solo ordenador en lugar de utilizar servidores especializados, todos ellos con sus propias necesidades de potencia, refrigeración y mantenimiento, es un argumento convincente. La utilización de varios nodos virtualizados alimentados a partir de un único servidor físico se traduce en ahorro empresarial. El efecto económico de la virtualización puede ser increíblemente potente: según una encuesta realizada por Forrester en 2011, la implementación de una infraestructura de escritorio virtual (VDI, del inglés "Virtual Desktop Infrastructure") de VMware ofrece un retorno de la inversión de un 255 % en un periodo de 4 años, alcanzando el umbral de rentabilidad 17 meses después de la implementación.

La pregunta es, ¿cuántas máquinas virtuales se pueden comprimir en esta configuración de hardware sin que el rendimiento se vea extremadamente afectado? Esto es lo que se conoce como el "índice de consolidación", y esto es lo realmente complicado debido a la gran cantidad de factores que se deben tener en cuenta. ¿Qué tipo de tareas son las que las máquinas virtuales deberían llevar a cabo? ¿Qué software de hipervisor se emplea? ¿Cuáles son los riesgos de poner todos los huevos en tan pocas cestas? Y por último, ¿cómo puede proteger de forma fiable su nueva infraestructura virtual, asegurándose de que no es vulnerable ante los cibercriminales, sin adoptar medidas extremas y frenar todo a paso de tortuga? Para tomar la decisión correcta, necesita comprender algunos conceptos y observar cómo funcionan de forma conjunta.

Modelos de virtualización

El sector ha definido varios modelos de virtualización. Este documento ha seleccionado tres:

- **Virtualización de servidores**: permite que varias instancias de un sistema operativo funcionen de forma conjunta en un solo servidor. Esta es la mejor manera de aumentar la utilización de los recursos, hasta un 80 % con respecto a un nivel medio de utilización de un 10-20 % en el caso de servidores físicos habituales de una sola función[1]. **Virtualización del hardware de los servidores**: ofrece un solo nivel intermedio (hipervisor) entre la máquina virtual (VM) y el metal. Ofrece un valor mayor que el de la **virtualización del software de los servidores**, donde el sistema operativo subyacente implica determinado consumo de recursos adicional. Para la mayoría de las aplicaciones empresariales se prefiere la virtualización de hardware.
- **Virtualización de escritorios**: ofrece un escenario de valor diferente mediante la sustitución de un grupo de escritorios físicos con la infraestructura de escritorio virtual (**VDI**). "Clientes ligeros" rentables, escritorios remotos basados en funciones, sucursales remotas sin necesidad de un servicio de IT especializado y todo el mantenimiento de cientos de lugares de trabajo limitado a varios servidores físicos.
- **Virtualización de aplicaciones**: en este caso, a diferencia de una infraestructura de escritorios remota basados en funciones; un entorno virtual se adopta solo para una sola aplicación. Para los enfoques de software como servicio, cada vez más populares, se trata de una elección natural y eficiente.

Todos los modelos de virtualización tienen muchos usos, y cada uno de ellos conlleva algunos riesgos importantes. Entre estos, el riesgo de las ciberamenazas es uno de los más importantes, por lo que es absolutamente necesario emplear algún tipo de solución de seguridad. Esta tarea se convierte en un reto aún más difícil al percatarse de que los tres enfoques se pueden emplear en el ámbito de una sola red de IT. Y, sí, también tendrá que hacer frente al consumo de recursos adicional.

---

[1] - *Ruest D. Virtualization. A Beginners Guide (Virtualización. Guía para principiantes). McGraw-Hill, 2010, página 4*

No obstante, existen formas de reducir el impacto en su infraestructura virtual recién creaday altamente eficiente.

Una solución de seguridad especializada para los entornos virtuales es esencial

Obviamente, puede instalar agentes de protección de endpoints familiares en sus máquinas virtuales. Pero a continuación enumeramos una serie de carencias importantes que pueden hacer que su experiencia con infraestructuras de IT virtualizadas sea mucho menos satisfactoria.

1. **Duplicación**. Cada máquina virtual tendrá un conjunto idéntico de componentes de seguridad, incluido un motor antimalware aislado y bases de datos de firmas, cada uno de los cuales tendrá que actualizarse de forma independiente. Por lo tanto, una parte significativa de sus recursos más preciados (potencia de procesamiento, memoria RAM y almacenamiento en disco) se consumirá de forma bastante inútil, reduciendo significativamente el índice de consolidación.
2. "**Tormentas**". Este término se utiliza para definir el análisis antimalware o la actividad de actualización de bases de datos simultáneos a través de varios equipos, que puede conducir a un repentino pico en el consumo de recursos y el consiguiente descenso del rendimiento, e incluso a una denegación de servicio. La configuración manual puede ayudarle a resolver parcialmente este problema, pero con tantos resultados y cientos de máquinas virtuales, la intervención manual puede ser una tarea que consuma muchísimo tiempo.
3. "**Brechas de seguridad instantáneas**". Algunas máquinas virtuales permanecen latentes hasta que se las activa cuando surge la necesidad. Por desgracia, no es posible actualizar los componentes ni las bases de datos de la solución seguridad en una máquina virtual inactiva. Por lo tanto, inmediatamente después del arranque y antes de que la actualización de seguridad se haya completado, la máquina virtual es vulnerable a un ataque.
4. **"Ataques de pánico".** Es una práctica común entre los administradores de sistemas predefinir la reacción a un brote de virus como el endurecimiento de los parámetros de seguridad, entrando en modo "paranoico" y desencadenando un proceso de análisis no programado. Una política de esta naturaleza, que puede ser valiosa para los nodos físicos, puede generar fácilmente una situación de estancamiento en un entorno virtual.
5. **Problemas de incompatibilidad.** Las máquinas virtuales son en muchos aspectos similares a sus homólogos físicos, pero existen algunas diferencias importantes a tener en cuenta, tales como el uso de los discos no persistentes o el proceso de migración de máquinas virtuales en caliente. Las soluciones antimalware estándar, que se han diseñado para endpoints físicos, no tienen en cuenta la gran variedad de matices característicos de los entornos virtuales, por lo que pueden causar retrasos y problemas técnicos inesperados, o incluso dejar de funcionar completamente.

Si tenemos en cuenta todos los puntos anteriores, la necesidad generalizada de una solución especializada es obvia. Un producto de este tipo debe crearse teniendo en cuenta todas las consideraciones anteriores y, al mismo tiempo, debe proporcionar el mayor nivel posible de protección con el mínimo impacto en el rendimiento general. Kaspersky Lab, el líder tecnológico mundial en el campo de la ciberseguridad, está a la altura de la labor, y ofrece una solución para las tres plataformas de virtualización más populares: VMware, Microsoft Hyper-V y Citrix.

Plataformas y modos de protección

Enfoque sin agentes

VMware, una de las plataformas de virtualización más antiguas y todavía de las más populares hoy en día, ofrece una solución llamada vShield, que permite que la máquina virtual no tenga que cargar con la tarea de disponer de bases de datos idénticas y agentes de análisis antimalware duplicados. Es lo que se denomina "enfoque sin agentes".

Kaspersky Lab ofrece una solución de seguridad especializada para plataformas VMware: **Kaspersky Security for Virtualization | Agentless.** En este caso, las funciones de análisis se transfieren a un único dispositivo virtual de seguridad (SVA, del inglés "Security Virtual Appliance"), una máquina virtual especializada en la que se encuentra tanto el motor de análisis como las bases de datos de seguridad, lo que proporciona protección para todas las máquinas virtuales que se ejecutan en el hipervisor.

Las ventajas son claras:

- La interfaz nativa de VMware vShield ofrece acceso eficiente a las máquinas virtuales, liberando recursos de máquinas individuales y asegurando la compatibilidad con otras tecnologías de VMware.
- Los recursos liberados debido a la concentración de las funciones antimalware y la base de datos de firmas en un único dispositivo virtual se puede utilizar ahora para implementar máquinas virtuales adicionales, lo que aumenta el índice de consolidación.
- Durante el arranque de las máquinas virtuales nuevas, la protección se proporciona al instante a través del SVA, sin "brechas de seguridad instantáneas" ni la necesidad de instalar ningún tipo de software adicional.
- El SVA siempre activo de Kaspersky mantiene su base de datos de firmas actualizada constantemente y, lo que es todavía más importante, mantiene la conexión con Kaspersky Security Network (KSN), una infraestructura mundial que procesa la información de millones de participantes voluntarios y ofrece protección contra las amenazas más recientes antes incluso de que se implementen a través de la actualizaciones de la base de datos.
- El problema de las "tormentas" desaparece mediante la actualización de un único SVA, que analiza automáticamente las máquinas virtuales mediante un programa establecido de manera aleatoria y a través de la limitación del número de subprocesos utilizados.

Además, con la ayuda de las funciones de seguridad de redes básicas proporcionadas a través de vCloud Networking and Security, la solución de Kaspersky puede detectar y prevenir los ataques entrantes en las máquinas virtuales, bloqueando eficazmente el atacante con la tecnología Network Attack Blocker [1].

Por desgracia, las capacidades de vShield son limitadas, ya que se proporciona acceso a las máquinas virtuales protegidas solo al nivel de los sistemas de archivos. Por lo tanto, los procesos que se producen dentro de la propia memoria de la máquina virtual no se pueden supervisar ni controlar por antimalware sin agentes. Esto significa también que otras tecnologías de endpoints, como el control de aplicaciones con marcado dinámico en lista blanca, diseñadas para ofrecer potentes niveles adicionales de seguridad, no se pueden implementar.

También cabe señalar que, como vShield es tecnología propiedad de VMware, el enfoque sin agentes para proteger una infraestructura virtual solo se puede aplicar de momento a la plataforma de VMware.

Enfoque de agente ligero

Conscientes de las limitaciones descritas anteriormente, **Kaspersky Lab** ofrece otra variante de solución para la virtualización, un enfoque que se encuentra a medio de camino entre el enfoque sin agentes y el enfoque de agente completo: **Kaspersky Security for Virtualization | Light Agent**.

Al igual que en el enfoque sin agentes, las bases de datos y el motor antimalware de análisis de archivos se encuentran en el SVA. Pero hay una diferencia: la implementación de un módulo residente ligero en cada una de las máquinas virtuales que se protegen.

Kaspersky Security for Virtualization | Light Agent no está limitado por las capacidades de seguridad de la tecnología vShield, pero tiene acceso directo completo a cada máquina virtual, incluido todo lo que sucede en el interior de cada memoria operativa. Por lo tanto, se puede emplear la gama completa de tecnologías de vanguardia de Kaspersky Lab para defender la infraestructura virtualizada.

Entre las ventajas clave de Kaspersky Security for Virtualization | Light Agent se incluyen las siguientes:

- Menos consumo de recursos en comparación con una solución de agente completo porque el motor de análisis de sistemas de archivos y las bases de datos se trasladan al SVA.
- Compatibilidad con las tres plataformas de virtualización más populares: VMware, Microsoft Hyper-V y Citrix*.
- El nivel más alto posible de protección, proporcionado por el acceso completo a los recursos de las máquinas virtuales, incluida la memoria operativa.
- Niveles adicionales de seguridad proactiva disponibles, tales como HIPS con prevención automática contra exploits y control de aplicaciones con marcado dinámico en lista blanca. Implementación sencilla incluso en los escenarios de seguridad más reforzados, incluido el de "denegaciones predeterminadas".
- La solución se diseñó desde el principio con la virtualización en mente, por lo que funciona con las funciones exclusivas del entorno virtual, no contra ellas.

Por supuesto, todo tiene un precio. El agente ligero debe estar presente en cada nueva máquina virtual implementada, un proceso que se puede automatizar fácilmente mediante la inclusión del agente ligero en la imagen de la máquina virtual generada previamente. Debido a la presencia del propio agente ligero, Kaspersky Security for Virtualization | Light Agent tiene un impacto ligeramente mayor en la memoria en comparación con la aplicación sin agentes, pero cabe decir que, en ciertas condiciones, la solución de agente ligero puede superar realmente a la aplicación sin agentes de vShield.

Un hecho más que debemos recordar es que el número de hipervisores compatibles está limitado por las tres plataformas más populares. Y, en el momento de la redacción de este documento, Microsoft Windows es el único sistema operativo invitado compatible con ambas aplicaciones (con agente y con agente ligero).

Sin duda eso no quiere decir que se encuentra indefenso si no emplea una de estas tres plataformas. Todavía no hemos hablado de la solución de seguridad de agente completo diseñada por Kaspersky Lab.

Enfoque de agente completo

Kaspersky Endpoint Security, a pesar de ser una solución de agente completo, en realidad es capaz de hacer muy buen trabajo en entornos virtuales. Aunque requiere más recursos que Kaspersky Security for Virtualization, se puede adoptar para su uso en entornos virtuales. Por lo tanto, si existe la necesidad de proteger una determinada configuración peculiar, ya sea un conjunto de servidores Linux o equipos Windows invitados en algún hipervisor exótico, aún estará protegido.

Entre las ventajas de la implementación de Kaspersky Endpoint Security en su infraestructura virtual se incluyen las siguientes:

- Compatibilidad con la mayoría de los sistemas operativos contemporáneos
- Incorporación del conjunto más completo de tecnologías avanzadas de Kaspersky Lab
- Principios de gestión totalmente familiares, como cualquier máquina física normal
- Tres agencias de consultoría líderes en el mundo (Gartner, IDC y Forrester) reconocen su eficiencia, denominándola una de las mejores plataformas de protección de endpoints: una "Triple Corona".

---

1 La configuración de la protección de redes en KSV | Agentless requiere la implementación de un SVA secundario

Tabla 1: Lista comparativa de funciones

Característica	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Plataformas de virtualización compatibles	VMware	VMware, Microsoft Hyper-V, Citrix	Cualquiera excepto a nivel de sistema operativo[1]
Sistema operativo invitado compatible	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Índice de consolidación dentro de un único host	* * *	* */* * *[2]	*
Gestión centralizada mediante Kaspersky Security Center	+	+	+
Funcionalidad de KSN	+	+	+
Protección de máquinas virtuales nuevas sin instalaciones adicionales	+	+/-[3]	-
Antimalware	* *	* * *	* * *
Firewall	-	+	+
Prevención de intrusiones basada en host (HIPS)	-	+	+
Network Attack Blocker	+	+	+
Control de aplicaciones con marcado dinámico en la lista blanca y compatibilidad con denegaciones predeterminadas	-	+	+
Control web	-	+	+
Control de dispositivos	-	+	+
Gestión de sistemas	-	+[4]	+[4]
Cifrado	-	-	+

Y ahora, después de todos los tediosos cálculos, se plantea una vez más la pregunta: ¿cómo obtener la máxima eficiencia sin ser vulnerables a las ciberamenazas? Pues existe un enfoque, que se puede utilizar como regla general, y se llama **seguridad basada en funciones.**

---

[1] – *Virtualización a nivel de sistema operativo, también llamada por zonas o contenedores; emplea un mecanismo donde muchos "contenedores" de espacio de usuario comparten un único kernel del sistema operativo. Paralelos y Proxmox son ejemplos de este tipo de plataformas.*

[2] – *Depende del hipervisor y el tipo de virtualización.*

[3] – *Para las máquinas virtuales no persistentes, la protección inmediata estará disponible una vez se haya incluido el agente ligero en la imagen de la máquina virtual. Para las máquinas virtuales persistentes, el administrador debe implementar el agente ligero manualmente.*

[4] - *Las tecnologías de valoración de las vulnerabilidades y gestión de parches, aunque en teoría están disponibles en Kaspersky Security for Virtualization | Light Agent, exigen muchos recursos y, por lo tanto, su uso no se recomienda en entornos virtuales.*

Bloqueo exclusivo de los golpes entrantes: un enfoque basado en funciones para la seguridad.

Cualquier ciberamenaza contra los endpoints físicos también puede poner en peligro la infraestructura virtual. Pero lo que es absolutamente necesario para un atacante es un método para penetrar el perímetro de seguridad para realizar un ataque. Por ejemplo, para infectar un PC en funcionamiento, puede que el cibercriminal necesite atraer al empleado al sitio web malicioso, donde la infección se produce a través de la explotación de una vulnerabilidad en el navegador de la víctima. Pero para infectar, por ejemplo, un servidor de bases de datos oculto en lo más profundo de la infraestructura de IT que posiblemente ni siquiera tenga conexión a Internet, se debe buscar otro vector de ataque. Por lo tanto, si está seguro de que las únicas amenazas posibles son las que atacan a los sistemas de archivos, que los datos en cuestión tienen poco valor por sí mismos o está utilizando VDI con políticas estrictas sin acceso a la web, puede optar por una solución sin agentes que ofrece las ventajas de protección instantánea y ausencia de "brechas de seguridad instantáneas".

Tabla 2: Enfoque de seguridad basado en funciones

Función	Acceso externo	Valor de los datos*	Valor del servicio**	Condiciones externas	Solución (Motivos para el uso de cierta solución)
Servidores de bases de datos back-end	No	Bajo a medio	Medio a alto	Copias de seguridad periódicas	KSV | Agentless (datos de corta vida, menos vectores de ataque)
Servidores web front-end	Sí	Bajo	Alto	Relaciones de confianza con varios back-end	KSV | Light Agent (Exposición a peligros de acceso público, es posible tras un ataque con éxito de explotación de confianzas)
VDI de finalidad limitada o aplicación virtualizada	No	Medio a alto	Medio	Muy restringidas, sin instalación de aplicaciones, sin uso de dispositivos de almacenamiento extraíbles	KSV | Agentless (Ambiente predecible, menos vectores de ataque)
VDI de sustitución de escritorio	Sí	Medio	Medio	Uso de dispositivos de almacenamiento extraíbles personales, usuarios privilegiados con derechos de instalación	KSV | Light Agent (La necesidad de un mayor nivel de seguridad es mayor que la necesidad de una respuesta rápida; más vectores de ataque debido a la exposición a Internet público)
Servidores web en intranet empresarial	Sí	Bajo a medio	Bajo a medio	*Acceso externo solo para los usuarios autorizados mediante tokens de hardware	KSV | Agentless (Poco valor comercial de los datos, una limitada exposición a Internet público)

Infraestructura de procesamiento de datos de clientes	Sí	Alto	Alto	Necesidad de un entorno estable y sin cambios; se recomienda control de aplicaciones con denegaciones predeterminadas	KSV | Light Agent (La necesidad de cumplimiento hace que los niveles adicionales de protección sean una necesidad absoluta)
Infraestructura de pruebas para desarrolladores web	Sí	Bajo a medio	Medio	Hipervisor basado en Linux y máquinas virtuales invitadas heterogéneas	KESB for Linux, KESB for Windows (Datos de corta vida constantemente renovados, variedad de sistemas operativos)

La tabla anterior muestra algunos ejemplos que ofrecen una comprensión general de las defensas basadas en funciones, aunque no es una recomendación directa para las funciones enumeradas y no debe utilizarse como tal. Cada caso es único, y siempre hay más condiciones que deben tenerse en cuenta y que no se pueden resumir en una sola tabla. No obstante, para que el concepto sea más claro, nos gustaría ofrecer la clasificación para el valor de los datos y el valor del servicio de forma más detallada:

- **Datos de valor bajo**: por lo general, estos datos están despersonalizados, no contienen secretos de valor personal, comercial o gubernamental valiosos, y tal vez sean de corta vida y objeto de constante renovación. Su pérdida o exposición no da lugar a importantes pérdidas comerciales y nunca pueden causar ningún daño a la reputación. Un buen ejemplo sería una base de datos laboral donde se almacenan temporalmente datos transitorios.
- **Datos de valor medio**: estos datos pueden contener alguna información personal o comercial, a excepción de los datos directamente relacionados con las finanzas y el bienestar personal. No contendrían información clasificada. Su pérdida puede causar algunos daños financieros a la empresa. Su exposición puede llevar a un notable impacto monetario y puede dañar la reputación de la empresa de forma no crítica. Ejemplo: datos sobre los clientes de un comercio online.
- **Datos de valor alto**: pueden contener información personal o financiera confidencial o secretos comerciales que constituyen una parte significativa de la ventaja en el mercado de la empresa. También pueden contener información clasificada. Su pérdida puede dar lugar a importantes pérdidas comerciales y de reputación. Su exposición puede llevar a graves sanciones financieras, incluidas demandas, y daños irrevocables en la reputación. Ejemplo: proyectos de algunas infraestructuras críticas o correspondencia confidencial entre ejecutivos.
- **Valor de servicio bajo**: no hay terceros afectados, la velocidad de recuperación es de poca importancia. Pocas consecuencias financieras o ninguna en caso de mal funcionamiento. La probabilidad de daños a la reputación es extremadamente baja. Ejemplo: portal de información empresarial.
- **Valor de servicio medio**: los terceros pueden verse afectados si el servicio no funciona correctamente. La pérdida de estos datos puede dar lugar a notables daños financieros. El daño a la reputación es notable también, y está directamente conectado a la importancia social del servicio: cuanto más conocido y popular sea el servicio (o el producto del que depende), más graves serán las consecuencias en lo que respecta a la reputación. Los datos pueden ser una parte de una infraestructura gubernamental, pero su condición tiene poca influencia sobre el bienestar nacional. La recuperación rápida es de vital importancia. Ejemplo: infraestructura de VDI de un integrador de sistemas que proporciona un entorno de sustitución de escritorios entre sus servicios.

- **Valor de servicio alto**: casi con toda seguridad hay terceros afectados. El servicio es el elemento clave de la empresa y puede ser un elemento crítico para terceros también. La influencia en el bienestar nacional es posible. Las pérdidas en lo que se refiere a la reputación son extremadamente dolorosas y pueden ser irrevocables. La recuperación es de suma importancia; si no se produce una correcta recuperación en el menor periodo de tiempo posible, pueden producirse más consecuencias dramáticas. Ejemplo: infraestructura de sistema de vigilancia por vídeo del gobierno.

Usted mejor que nadie conoce su infraestructura, por lo tanto, es quien mejor puede decidir cuál es el grado de seguridad que necesita; las directrices que hemos indicado aquí son solo eso, una metodología básica para tomar una decisión. Pero sí, es bastante posible mejorar la eficiencia en la utilización de recursos y ahorrar un poco de dinero para su empresa a la vez que mantiene su infraestructura virtual segura. No obstante, recuerde que antes de implementar cualquier tipo de solución de seguridad especializada, debe comprobar y ajustar la configuración de seguridad básica de la red de IT. Una red administrada correctamente se traduce en menos vectores de ataque para los criminales y menos consecuencias negativas si algo sale mal.

Eficiencia significa integridad

Un uso eficiente de los recursos está bien, pero no es nada sin un control eficaz. Sin duda se puede implementar una solución sin agentes para sus back-end de un proveedor, una solución de agente ligero para su VDI de otro proveedor y aplicar el control de aplicaciones de terceros para algún área crítica. Como resultado, dispondrá de tres consolas de gestión, tres conjuntos de políticas que deberá configurar y mantener, y determinado tráfico de actualización excesivo que deberá pasar a través del canal de datos. Desde luego, es mucho mejor que todo provenga de un único proveedor, con todos los indicadores y controles perfectamente organizados en una sola consola. Todos los productos de seguridad de Kaspersky se han diseñado para controlarse de forma centralizada, a través de Kaspersky Security Center. Esto significa que puede administrar sus activos virtualizados desde la misma consola que emplea para controlar la seguridad de los endpoints físicos.

Otra ventaja es la actualización centralizada. No hay necesidad de descargar el mismo conjunto de actualizaciones para cada SVA en cada hipervisor; se implementan de forma automática una vez descargados en el sistema de almacenamiento de KSC.

Otra característica distintiva de las soluciones de Kaspersky Lab es su disponibilidad para distintas plataformas de virtualización. Por lo tanto, puede gestionar un entorno con varios hipervisores bien protegido y, aún así, disfrutar de la centralización de todos los controles en KSC.

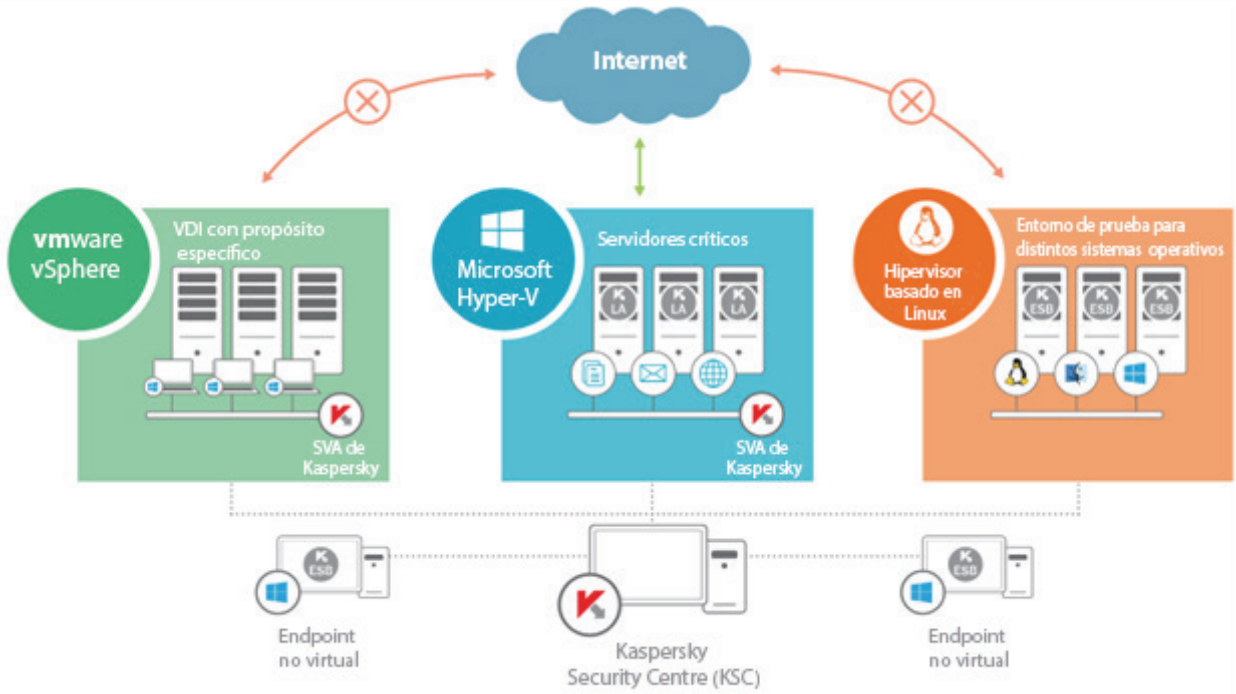

Figura 1: Un entorno con varios hipervisores se puede proteger de manera sólida y eficiente

Por ejemplo, el núcleo de Active Directory (controladores de dominio, sistemas de nombres de dominio, etc.) puede estar alojado en servidores virtuales Microsoft Hyper-V, emplear un VDI de Citrix e incluir algunos servidores de bases de datos en VMware ESXi. O bien, como se muestra en la figura anterior, puede gestionar un entorno mixto que contenga una plataforma de varios hipervisores y endpoints físicos.

En este caso, para obtener el equilibrio más eficiente entre rendimiento y seguridad que conduzca a índices de consolidación óptimos:

- KSV | Agentless puede proteger un VDI con propósito específico aislado
- La infraestructura de servidor que sea de importancia esencial para las empresas y contenga datos valiosos debe protegerse con niveles de seguridad sólida de KSV | Light Agent
- El entorno de prueba, con el hipervisor de Linux y un zoológico de sistemas operativos invitados y endpoints físicos, está mejor protegido por Kaspersky Endpoint Security.

En todo caso, los productos de Kaspersky Lab le ofrecen la mejor protección que ofrece el sector, y le permiten elegir entre una implementación fácil y la eficiencia en el retorno de la inversión de la solución KSV | Agentless, la sólida protección de KSV | LA o cualquier otra combinación en una sola infraestructura de IT.

Como Kaspersky Lab puede ofrecer a los clientes soluciones de virtualización sin agentes, con agente ligero y basadas en agentes, podemos hacer recomendaciones completamente objetivas a nuestros clientes. No tenemos la necesidad de promocionar ninguna tecnología específica, pero podemos sugerirle la mejor opción, o combinación de opciones, para un entorno de cliente específico. Y como todas nuestras soluciones se basan en el mismo potente motor antimalware, y todas ellas están diseñadas por nosotros como parte de una única plataforma de seguridad integrada, sabemos que la opción que elijas funcionará de manera eficiente para mantener su sistema virtual seguro.